THE CASE FOR SPACECRIME:
THE RISE OF CRIME AND PIRACY IN THE SPACE DOMAIN

BY

MAJOR ANDREW J. EMERY

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2013

Report Documentation Page	Form Approved OMB No. 0704-0188

1. REPORT DATE **JUN 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **The Case for Spacecrime: The Rise Of Crime And Piracy In The Space Domain**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Crime exists in a symbiotic relationship to humanity: wherever people aspire to lawful enterprise, criminals endeavor to achieve illicit gains. Whether on land, on the sea, in the air, or through cyberspace, criminal activity quickly joins legitimate commerce in every domain of economic activity. So why is there no crime in space?

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**66**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards or research, argumentation, and expression.

EVERETT C. DOLMAN, PhD

MICHAEL V. SMITH, Col, USAF, PhD

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Andrew Emery was born and raised in Cincinnati, Ohio, and received his commission through the Reserve Officers Training Corps at Rose-Hulman Institute of Technology in 1999. His first assignments were at Randolph AFB and Brooks AFB, Texas, where his greatest accomplishment was meeting and marrying his wife.

He continued to Los Angeles AFB, where he directed ground and on-orbit testing for the first modernized Global Positioning System (GPS) Block IIR-M satellite. He was selected for an operational exchange tour, was assigned to the 2d Space Operations Squadron at Schriever AFB, and culminated his tour as GPS Mission Analysis flight commander.

After a year at Headquarters Air Force Space Command at Peterson AFB managing senior leader assignments, he was selected for the Air Force Strategic Policy Intern program at the Pentagon. During this yearlong fellowship, he worked in the Joint Staff J-5 Director's Action Group and in the Air Force Legislative Liaison Office. He moved to SAF/AQR, the organization responsible for managing Air Force Research and Development, where he led several programs.

He holds a Bachelor of Science degree in Computer Engineering from Rose-Hulman Institute of Technology, and a Master of Science degree in Systems Architecture and Engineering from the University of Southern California. Following his assignment as a student at the School of Advanced Air and Space studies, he will be assigned to the Strategy Division of the Joint Space Operations Center (JSpOC) at Vandenberg AFB.

ACKNOWLEDGEMENTS

My gratitude goes to the faculty and staff at SAASS. Their dedication to the SAASS mission and curriculum fulfilled the legend, as did their ability to decimate students' misplaced self-confidence while simultaneously inspiring them to learn. I am grateful for the many hours of instruction and mentoring I received…it was excruciatingly worth it.

I also want to express my indebtedness to my fellow classmates. I have never been so challenged, so humbled, and so encouraged in my Air Force career. The conversations evolved my perceptions of airpower, security studies, leadership, strategy and a host of other topics. Our interactions in the classroom, hallway, kennels, and especially the Legacy Room were central to my positive SAASS experience.

Finally, I need to thank my family for their sacrifices to help me succeed this past year. My daughter's inexhaustible toddler energy and unwavering greetings at the door each evening served to invert my seemingly unending surplus of frowns. Most importantly, if not for my wife's herculean efforts managing our home, her constant encouragement, and her gracious and (usually) gentle prodding, I would not have endured the year. Her love is indisputable, unfailing, and eternal…and that makes me the luckiest man around.

ABSTRACT

Crime exists in a symbiotic relationship to humanity: wherever people aspire to lawful enterprise, criminals endeavor to achieve illicit gains. Whether on land, on the sea, in the air, or through cyberspace, criminal activity quickly joins legitimate commerce in every domain of economic activity. So why is there no crime in space?

Criminology theories offer the insight needed to address this question. One of those theories—Routine Activity Theory—contends that crime occurs when motivated offenders, suitable targets, and a lack of capable guardians converge in time and place. In this thesis, spacecrime refers to those acts undertaken in or from space for primarily financial gain. First, I analyze the efforts required for motivated and capable offenders to build and launch a satellite they can use to commit spacecrime. Next, I examine the space commerce sector to determine whether suitable targets exist to entice offenders. Finally, I explore the state of guardianship in space: who is able to monitor space, and what actions can they take to prevent crime?

I conclude there are plenty of viable targets, and that guardianship is inadequate: even with sufficient passive monitoring, the ability to respond to crime in space is extremely limited. The primary reason for a lack of spacecrime is the difficulty and cost associated with becoming a criminal—the technology and launch costs are still too high. However, my research revealed that small satellite technology is rapidly becoming more lightweight, modular, and cheaper, and that access to space over the next decade will be easier and less expensive than today. A time will come when the cost/benefit analysis will motivate offenders to undertake spacecrime, and it will prove to be profitable. Therefore the international community should address possible mitigation and prevention policies now, rather than waiting for the first criminal act.

CONTENTS

INTRODUCTION

Crime is ubiquitous. It exists regardless of where an offender or victim resides along the socioeconomic spectrum, and manifests anywhere along a continuum of violence. Crime for economic benefit crosses domains—land, sea, air and cyber. From shoplifting at a retail store to piracy off the Somali coast; from hijacking of aircraft to identity theft via the Internet, men and women endeavor to redistribute wealth from others to themselves through criminal enterprise. The variety of possibilities is endless, ranging from petty gains by impetuous individuals to quasi-corporate international criminal organizations. If humans have sought to achieve illegal financial gain in all other domains, why has crime not yet migrated to space?

In this thesis I focus specifically on *economic crime*—those criminal acts carried out by individuals or groups with the primary purpose of financial gain. These types of criminal acts take a myriad of forms: kidnapping, ransoming, hijacking, theft, money laundering, and a host of others. While other categories and types of crime are possible in space, I chose to restrain from my investigation those acts undertaken for a primary purpose other than economic benefit.

The majority of space policy and international arms control efforts focus on state actors and their interactions with one another, or with non-state actors and the threat of terrorism. The subject of criminal interaction between private entities is considered scarcely, if not ignored completely, in public discourse. The reason for this is simple: it has not yet happened. Contrasted with issues of maritime piracy and cybercrime that clamor for immediate responses, the question of crime in space falls through policy seams quite easily.

In this thesis I examine the act of crime itself—the factors which, when present, generally permit crime to occur—and utilize a criminology theory to investigate crime in the space domain. Routine Activity Theory

contends that when motivated and capable offenders, a supply of suitable targets, and a lack of capable guardianship converge within a given domain in time and place, crime will occur. Manipulating any of these three factors can affect directly the amount of crime that may arise.

The purpose of this thesis is to analyze the topic of spacecrime utilizing this theoretical framework, determine its likelihood of occurrence, and recommend further areas of study to progress this issue from the fringe into mainstream policy discussions. If crime does occur in space, it will present problems to the international community analogous to maritime piracy and other transnational crimes, and will consequently require an international response. Although it has not yet occurred, and may not occur for another decade or more, discourse on international policy and law should address spacecrime now.

The first chapter provides an overview of general theories of crime and introduces Routine Activity Theory. I discuss in detail the three primary factors: offender, target, and guardian. I demonstrate how Routine Activity Theory offers value toward understanding crime in the maritime and cyberspace domains, and explain why it is useful in forecasting the rise of spacecrime.

In the second chapter, I apply Routine Activity Theory to the space domain, investigate why crime has not yet occurred there, and identify the factors, which if modified, would allow for the rise of spacecrime. Although the conditions of a lack of capable guardianship and supply of suitable targets in space are currently met, the supply of motivated and capable offenders is lacking. This supply is likely to grow as non-state and individual actors increase their presence in space. This increase will occur as technology continues to improve, and the costs decrease for both improved satellite technology and space transportation.

The final chapter offers conclusions and some recommendations for further study. My goal for this thesis is not to conduct a broad review of current international policy and law, to provide a solid business case

for criminal enterprise in space, nor to offer specific recommendations on how to control or prevent space crime. Rather, the scope of this thesis is the argument that crime in space is analogous to crime in other domains and, given the right conditions, will arise and require a response. My investigation concludes that those conditions are likely to be met, and therefore the problem of spacecrime is worthy of increased consideration by policymakers today.

CHAPTER 1

Routine Activity Theory: An Introduction

There are crimes of passion and crimes of logic. The boundary between them is not clearly defined.

Albert Camus
The Rebel: An Essay on Man in Revolt

Why does crime occur? This question has plagued humanity since its beginning, and whether it is the *right* question is subject to debate. Looking solely at criminal behavior prompts a different question: why do people commit crime?[1] Studying characteristics of the criminal aggregate leads to analysis beyond the choices of individuals, and to questions such as: why do people raised in particular locations, or under certain conditions, or with similar backgrounds, have a higher probability of committing crime? These questions yield to those aimed at society's response: how does society prevent crime and protect its law-abiding citizens? Theories of explanatory and preventive nature abound, and seek generally to reduce criminal motivation through education or reform, safeguard victims and property through various protection mechanisms, or directly prevent criminal activity through active employment of security or law enforcement officers.

These theories of crime are divided into two broad categories—those that examine the development of *criminal offenders*, and those that attempt to explain *criminal events*.[2] Offender-based theories are further divided into individual and sociological categories, although the lines

---

[1] Robert Agnew, *Why Do Criminals Offend? A General Theory of Crime and Delinquency* (Los Angeles, CA: Roxbury, 2005).

[2] John E Eck and David Weisburd, *Crime and Place*, vol. 4, Crime Prevention Studies (Monsey, NY: Willow Tree Press, Inc., 1995).John E Eck, David Weisburd, and Police Executive Research Forum, *Crime and Place* (Monsey, NY; Washington, DC: Criminal Justice Press; Police Executive Research Forum, 1995).

between these distinctions are easily blurred.[3] Individual theories attempt to explain criminal behavior by examining the motivations of individual offenders. Sociological theories examine an offender's physical, cultural, and social environment, and attempt to explain criminal behavior in light of these socioeconomic factors. Both groups of theories seek to explain crime through the lens of the criminal, and are fertile ground for debates on the nature of humanity, how its characteristics are altered by various factors, and how society can manipulate these factors to decrease or prevent criminal behavior.

Theories focused on the criminal event itself purposely marginalize the characteristics of offenders, and attempt to identify the circumstances under which crime occurs independent of the offender's attributes. These structural theories offer the opportunity to anticipate the conditions most conducive to criminal behavior without focusing on the uncertainty of human motivation, morality, ethics, or the complexity and diversity of sociological and environmental factors. Although all theories of crime are theories of human behavior at their root—therefore strictly contextual and generally limited—some are nonetheless useful.[4] No theory of crime extends perfectly to the space domain, primarily because criminologists focus their research on the plethora of criminal activity on earth. However, since structural theories minimize the *who* and *why* in the crime equation, and thus the sources of greatest uncertainty, they offer the best option to explore criminal events in a domain where they have not yet occurred.

Within the area of structural theories, a branch of economic crime analysis grew from Nobel laureate Gary Becker's seminal article

---

[3] Thomas J. Bernard, *Vold's Theoretical Criminology*, 6th ed (New York: Oxford University Press, 2010).

[4] George E. P. Box, *Empirical Model-building and Response Surfaces*, Wiley Series in Probability and Mathematical Statistics (New York: Wiley, 1987), 424. Dr. Box recognized that "...all models are wrong, but some are useful."

published in 1968.[5] Rather than focusing on the then-predominant approach of researching criminal motivation, Becker developed a model that viewed criminal activity as a rational choice alternative to generating legal income.[6] This cost/benefit analysis included alternatives to legitimate work, the availability of economically viable targets, and the ability to succeed in criminal enterprise without repercussion.[7] Although on the surface this appears to offer another theory of criminal offenders, its focus was not the individual criminal, but rather the criminal aggregate—as long as crime offers an opportunity for financial gain, some people will choose to commit criminal acts rather than, or in addition to, legitimate work.[8]

Building on this foundation, crime becomes less of a problem that can be eradicated, and more of an inexorable element of society—just one of many variables in the economic calculus of human existence. Given the option of a crime-free world in a utopian sense, most people would choose to live in such a world. However, in a real world populated by self-interested humans, achieving a crime-free world is not fiscally feasible. The tremendous amount of resources required, coupled with the restrictions of civil liberties required to achieve zero crime, would be unpalatable to most people.[9] In other words, there cannot be an absence of crime without an excess of cost.

So the question remains—why does crime occur? An economics-based theory is not the *only* way to consider crime, nor necessarily the

---

[5] Gary S. Becker, "Crime and Punishment: An Economic Approach," *Journal of Political Economy* 76, no. 2 (January 1968).

[6] Helen Tauchen, "Estimating the Supply of Crime: Recent Advances," in *Handbook on the Economics of Crime*, by Bruce L Benson and Paul R Zimmerman (Northampton, MA: Edward Elgar, 2010), 24.

[7] Bill McCarthy, "New Economics of Sociological Criminology," *Annual Review of Sociology* 28, no. 1 (August 2002), 417–442.

[8] Becker, "Crime and Punishment."

[9] Harold Winter, *The Economics of Crime: An Introduction to Rational Crime Analysis* (New York: Routledge, 2008):8.

best, but it is extremely useful. It helps explain why crime might come to exist in a given domain, independent of the individuals who carry out the criminal act. This thesis does not aim to provide a definitive rationale for why crime exists or how to eliminate it, but rather to examine one theory's explanation for crime, and how this applies to the only domain without criminal activity—space. Routine Activity Theory, a structural-based economic theory of crime, provides such an explanation.

Overview of Routine Activity Theory

Lawrence Cohen and Marcus Felson developed Routine Activity Theory in the late 1970's, and published it in *The American Sociological Review* in 1979.[10] It assumes a rational choice approach, where an offender utilizes a deliberate cognitive process to select the type of crime to commit, choose the target victim, decide upon the time and place of the criminal act, and calculate the probability of apprehension.[11] If the benefit outweighs the risks involved, the offender will choose to perpetrate a criminal act. The focus of their research was "direct-contact predatory crime," in which someone "takes or damages the person or property of another."[12] They argued the structure of the routine activities of everyday life affect the amount of crimes committed. The focus of their theory is on the criminal act itself, the variables required to enable such an act, and assumes criminal inclination is a given.[13]

Cohen and Felson create a framework of three minimal criteria to explain why crimes take place: a motivated and capable offender, a

---

[10] Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, no. 4 (August 1979), 588.

[11] Cohen and Felson, "Social Change and Crime Rate Trends," 588-608; T. Burke, "Routine Activity Theory," in *The Praeger Handbook of Victimology*, ed. Janet K. Wilson (Santa Barbara, CA: Praeger, 2009), 232–233.

[12] Daniel Glaser, *Social Deviance* (Cambridgeshire, UK: Markham Publishing Company, 1974), 4.

[13] Cohen and Felson, "Social Change and Crime Rate Trends," 589.

suitable target, and an absence of capable guardians.[14] The convergence in space and time of these three elements, or the lack of any single one, is sufficient to explain an increase or decrease in crime rates.[15] By understanding the dynamics of each element, officials can better explain and influence criminal activity by manipulating the ratio of offenders to targets, targets to guardians, or guardians to offenders.[16]

Offenders must be motivated and capable of committing a criminal act. The source of motivation under Routine Activity Theory is irrelevant: whether financing a drug habit, feeding one's family, fueling a need for thrills, or succumbing to peer pressure, the final result is a motivated offender willing to commit a crime.[17] *Criminal offender*-based theories of crime focus heavily on the area of motivation.[18] Arguably more important is an offender's *capability* to complete the criminal act, and to do so without apprehension. Although many people might be willing to rob a bank, few have the ability to do so without getting caught. But unsuccessful bank robberies still occur, and it is not likely that offenders can be prevented from attempting crimes.[19] This element of Routine Activity theory is the nexus of individual motivations, skills, and aptitude, and is related closely to finding suitable targets.

A suitable target can be a person or an object.[20] The target must prove both vulnerable and desirable to the offender. Factors such as target location, lifestyle, socioeconomic status, culture, and habits play a role in victim selection. For instance, if an offender wishes to burglarize

---

[14] Cohen and Felson, "Social Change and Crime Rate Trends," 589.

[15] Cohen and Felson, "Social Change and Crime Rate Trends," 589.

[16] Cohen and Felson, "Social Change and Crime Rate Trends," 604.

[17] Glaser, *Social Deviance,* 58.

[18] Eck and Weisburd, *Crime and Place*, 5.

[19] Ronald V. Clarke and David Weisburd, "On the Distribution of Deviance," in *Policy and Theory in Criminal Justice: Contributions in Honour of Leslie T. Wilkins*, by Don Gottfresdon (Aldershot, UK: Avebury, 1991).

[20] Cohen and Felson, "Social Change and Crime Rate Trends," 590.

a home, the choice is most likely one that provides easy entry, does not contain a security system, does not have large dogs, whose owners follow a daily routine, etc.[21] In addition, a home that contains expensive electronics, computers, jewelry, and other valuable goods is more desirable than one of little value. When vulnerability and value combine, it increases the suitability of a target, and without guardianship the likelihood of becoming a victim grows.

Capable guardians serve by simple presence to deter criminal activity, and by absence make crime more likely.[22] Security guards and law enforcement officers are formal examples of guardians, but neighbors, parents, and even strangers in the area can serve to discourage an offender.[23] Security cameras also serve as a form of passive guardianship, since their presence implies a watchful human on the other end of the lens. A lack of guardianship directly influences an offender's calculation of the probability of apprehension. Cohen and Felson posit that when motivated offenders and suitable targets converge in time and space, the presence or lack of guardianship is directly related to the probability of a criminal act transpiring.[24]

Using this framework, Cohen and Felson examined crime rates after World War II in an attempt to explain why crime rates were higher than before the war, despite America's economic prosperity. Their analysis concluded that macro-level factors—such as unemployment rates and national economic prosperity—were less important for explaining crime rates than the three criteria of Routine Activity Theory.[25]

---

[21] Lawrence E. Cohen, Marcus Felson, and Kenneth C. Land, "Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977," *The American Journal of Sociology* 86, no. 1 (July 1980): 90.

[22] Marcus Felson, "Those Who Discourage Crime," in *Crime and Place: Crime Prevention Studies*, eds. J. E. Eck and D. Weisburd, (St. Louis, MO: Willow Tree Press, 1995): 53.

[23] Cohen and Felson, "Social Change and Crime Rate Trends," 592.

[24] Cohen and Felson, "Social Change and Crime Rate Trends," 589.

[25] Cohen and Felson, "Social Change and Crime Rate Trends," 604.

They concluded “the convergence in time and space of suitable targets and the absence of capable guardians can lead to large increases in crime rates without any increase or change in the structural conditions that motivate individuals to engage in crime.”[26] In other words, no matter how good an economy is or how many jobs are available, people still choose to commit crimes based on internal, rational choice decisions. Whether this rational choice is intelligent or logical is immaterial—given the existence of the three factors, crimes will occur.

Routine Activity Theory has matured since its introduction, and several others have made enhancements. John Eck introduced a three-fold model of supervision to supplement the element of guardianship. In his model, guardians serve to protect targets, handlers influence offenders, and managers supervise places.[27] *Guardians* could include friends (such as running with another person through a park for mutual protection), or formal security through guards or law enforcement officers.[28] When people or objects are separated from guardians for prolonged periods of time, the likelihood of becoming a target increases.[29] *Handlers* are people with direct contact and influence over an offender, including parents, teachers, friends, or employers.[30] *Managers* are those who supervise the *places* where crime might occur, and include janitors, building managers, and store employees. In order for an offender to commit a criminal act, a handler or manager must be absent, ineffective, or negligent.[31]

---

[26] Cohen and Felson, “Social Change and Crime Rate Trends,” 604.

[27] John E. Eck, “Drug Markets and Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing” (Doctoral Dissertation, University of Maryland, 1994).

[28] John E. Eck and David Weisburd, *Crime and Place*: *Crime Prevention Studies* (Monsey, NY: Willow Tree Press, Inc., 1995), 5.

[29] Felson, “Those Who Discourage Crime,” 55.

[30] J. E. Eck and D. Weisburd, “Crime Places in Crime Theory,” *Crime and Place: Crime Prevention Studies* 4 (1995): 5.

[31] Eck and Weisburd, “Crime Places in Crime Theory,” 6.

These structural elements provide the necessary conditions with which to study the occurrence of criminal activity in general. The convergence in time and place of motivated and capable offenders (without handlers), a supply of suitable targets (without guardians), and a lack of capable place supervision (without effective managers) presents a broad theoretical framework with which to examine criminal activity in multiple domain contexts. The remainder of this chapter will analyze Routine Activity Theory's ability to explain and predict economic crimes in the global commons.

Routine Activity Theory Applied to Other Domains

The utility of Routine Activity Theory comes through its broad transfer value and applicability beyond the terrestrial domain.[32] All theories are incomplete and therefore only partially valid, but nevertheless provide useful functions when they define, categorize, explain, connect, and anticipate.[33] In order to extend Routine Activity Theory beyond its original context, the following section utilizes Harold Winton's theoretical taxonomy to clarify how the theory applies to case studies in the maritime, cyberspace, and space domains.

The first task is to define the scope of Routine Activity Theory in the context of this thesis.[34] While Cohen and Felson applied the theory to crimes against persons and objects, it was not limited to crimes of this type, nor to crimes for economic benefit alone.[35] This thesis focuses specifically on *economic crime:* those criminal acts carried out by individuals or groups for the primary purpose of financial gain. In addition, although the threat of violence might be employed in some

---

[32] JC Wylie, *Military Strategy : A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), 31.
[33] Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession," *Journal of Strategic Studies*, no. 6 (2011): 857.
[34] Winton, "An Imperfect Jewel," 854.
[35] Cohen and Felson, "Social Change and Crime Rate Trends," 590.

circumstances, these crimes are generally non-violent in nature. These types of criminal acts may take a myriad of forms: kidnapping, hijacking, ransoming, theft, money laundering, etc. While other forms of crime are certainly possible, this thesis excludes those acts undertaken for a primary purpose other than economic benefit.[36]

The next step is to examine how the constituent parts of Routine Activity Theory—offender, target, and guardian—apply in the context of the global commons. The assumption that *some* capable offender will arise who is willing to commit a crime, regardless of intervening factors, still applies. Offenders must also possess the requisite technical knowledge and capability to commit the criminal act. This includes equipment and supplies, background information on the target, foundational knowledge, etc. For example, a maritime pirate must possess a ship and weapons, have a basic understanding of maritime operations and navigation, know which ship to target and where it is located, and understand how to impose a ransom and receive payment. In most cases, offenders require some amount of financial backing to support their crime. This might come through personal investment, criminal organizations, or via state funding. Offenders also require physical access to the target, even in the case of cybercrime. Although an offender might use virtual means to commit a cybercrime, the target is still accessed and affected in the real world.

A target contains four properties that affect an offender's assessment of its suitability: value, inertia, visibility, and accessibility.[37] In general, value refers to the intrinsic worth of a target to the offender. This value need not be financial, but for the purpose of this thesis *value*

---

[36] While some scholars consider maritime piracy as terrorism, any piracy carried out for the economic benefit of the offender(s) is considered economic crime, rather than a terrorist act, for the remainder of this thesis.

[37] Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *European Journal of Criminology*, no. 4, (October 1, 2005): 419.

refers to the economic benefits perceived through undertaking a criminal act against a given target. *Inertia* refers to the physical characteristics of a target—volume, mass, velocity—and their contextual effect on whether a target is worth pursuit.[38] *Visibility* is critical, since offenders must know a target exists, and be able to locate it.[39] Offenders must possess enough information about a target to locate it, and in the case of a moving target, to track and predict its future location. Finally, *accessibility* refers to the "ability of an offender to get to the target and then get away from the scene of a crime."[40] This includes the concept of anonymity, and the overall judgment of whether crime against a given target is possible without apprehension.[41] The suitability of a target is a composite of these four characteristics, combined with an assessment of whether a given target possesses competent guardians.

Guardians must be capable of preventing crime from occurring.[42] Prevention is possible through direct action, or merely by the physical presence of the guardian.[43] Routine Activity Theory suggests mere presence is sufficient in many cases to remind a potential offender that someone is looking.[44] The crux of guardianship is presence *at the time* a motivated and capable offender converges with a suitable target.[45] This is the challenge for guardianship of the global commons—the ability to monitor and engage potential offenders or targets *at the proper time.* At

---

[38] Yar, "The Novelty of Cybercrime," 420.

[39] Richard R. Bennett, "Routine Activities: A Cross-National Assessment of a Criminological Perspective," *Social Forces*, no. 1 (September 1, 1991), 148.

[40] Marcus Felson, *Crime and Everyday Life*, 2nd ed. (SAGE Publications, Inc, 1998), 58.

[41] Yar, "The Novelty of Cybercrime," 421.

[42] Andromachi Tseloni et al., "Burglary Victimization in England and Wales, the United States and the Netherlands A Cross-National Comparative Test of Routine Activities and Lifestyle Theories," *British Journal of Criminology*, no. 1 (January 1, 2004), 74.

[43] Lawrence E. Cohen, Marcus Felson, and Kenneth C. Land, "Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977," *The American Journal of Sociology*, no. 1 (July 1980), 97.

[44] Felson, *Crime and Everyday Life*, 53.

[45] Yar, "The Novelty of Cybercrime," 423.

sea, in cyberspace, and in space, the idea that mere presence of bystanders is suitable to deter crime is insufficient. Guardianship of the global commons is therefore likely to be formal rather than informal, consisting of professionals tasked for the duty and capable of taking direct action.

With these components in place, Routine Activity Theory offers a framework for the etiological analysis of crime in various domains. Regardless of criminal motivation, criminal acts take place when capable offenders have a supply of suitable targets from which to choose, and when those targets lack sufficient guardianship. The theory has been used primarily to explain why crime *has* occurred, and what actions are possible to prevent crime by decreasing offenders, suitability or supply of targets, or increasing or improving guardianship. But the theory is also useful to explain why crime *will* occur, using the three core variables. If a car is left unlocked with the keys in the ignition, in a location where offenders have stolen many cars, and where the police patrol infrequently, it is highly probable the car will be stolen. This anticipatory value extends not only to domains where crime has occurred in the past, but also to the space domain where crime has yet to occur.

My primary purpose is to investigate the anticipatory applicability of the theory to the space domain by appraising the current status of capable offenders, suitable targets, and lack of guardianship. Many potential business cases support criminal ventures in space, but for simplicity this thesis focuses on one: hijacking and ransoming a target satellite using an offender's satellite. Examining the current status of each category will answer the question: why has crime in space not yet occurred?

My goal in utilizing Routine Activity Theory is not to predict the exact conditions required for crime in space, the nature of the criminal actor, nor provide specific solutions for avoiding or preventing this criminal activity from occurring. The goal is to demonstrate that

spacecrime is a real possibility, and requires serious consideration by policy makers. Unless action is taken in the near-term to reduce the potential for criminal offenders in space, decrease suitability of targets, or increase the effectiveness of guardianship, spacecrime will be unavoidable.

CHAPTER 2

The Case for Spacecrime

You look at these scattered houses, and you are impressed by their beauty. I look at them, and the only thought which comes to me is a feeling of their isolation and of the impunity with which crime may be committed there.

Sir Arthur Conan Doyle
The Adventure of the Copper Beeches

A civilian space industry encompassing commercial activity did not exist before the formation of the National Aeronautics and Space Administration (NASA) in 1958. Prior to this time, the Department of Defense (DOD) led and carried out research into space technologies.[1] The US government's decision to contract with a fledgling industry for civilian space programs provided a means for the sector to grow. With the launch of the first commercial satellite on July 10, 1962, outer space joined the global commercial domains of sea and air.[2] Although the race to the moon captured the world's hopes and dreams, the economic opportunities in space promised to capture its pocketbooks. The race to commercialize and profit from space had begun.

The entire commercial space economy was estimated as a $189.4 billion industry in 2011.[3] The commercial space products and services sector—the target for spacecrime in the context of this thesis—collected $102 billion in revenue. One industry report categorizes this sector into the broadcasting, communications, earth observation, geolocation and

---

[1] Henry R. Hertzfeld, *Space Economic Data 2002,* United States Department of Commerce, Office of Space Commercialization, 9, http://www.space.commerce.gov/library/reports/2002-12-economic-data.pdf.
[2] United States Space Objects Registry, "Details of Telstar-1," http://usspaceobjectsregistry.state.gov/registry/dsp_DetailView.cfm?id=90
[3] Space Foundation, *The Space Report 2011: The Authoritative Guide to Global Space Activity* (Colorado Springs, CO: Space Foundation, 2011), 6. This number represents the global space economy estimates minus the amount spent for US and non-US governmental programs.

navigation, space transportation, and in-space activities subsectors.[4] The goal of spacecrime is to redistribute wealth created from this industry into the pockets of successful offenders. The role of this industry in affecting the cost/benefit analysis of potential offenders is discussed later in the chapter.

Spacecrime could consist of many possible actions, limited only by the criminal imagination. For the purpose of thesis, in order to contain the topic and to narrow the analysis considerably, *spacecrime* is limited to criminal acts undertaken by an individual or group *from* space against a target *in* space, primarily for financial gain. While spacecrime could include nefarious acts *into* space from other domains, or *from* space into other domains, the terse limitation here proscribes digressions into definition or tangential analysis. Specifically, an offender must possess the technical skills required to build and operate a satellite, and gain access to space via some launch service provider; the target must be suitable enough to meet the offender's cost/benefit calculation; and guardianship must be insufficient to the point of emboldening an offender to act.

Spacecrime is not, for example, simply jamming a satellite from the ground. This may have occurred in a limited fashion already, but has proven ineffective as a successful extortion method since it requires the jammer to be in constant line of sight to its target. In the case of LEO targets this presents a challenge: if the jammer can only see its target for a short period of time, then it cannot continuously deny access to the target's operator. Targets in GEO are more susceptible to terrestrial jamming, since a single jammer can maintain line of sight to its target, and could therefore deny access continuously. However, unless the jammer is mobile or the offender employs multiple jammers at different locations operating at different times, the locations of persistent jammers

[4] Space Foundation, *The Space Report 2011*, 35–41.

are eventually discovered. At least one private company provides the resources and means to do so, including the use of helicopters and sensitive electronic gear to geolocate the jamming source.[5]

Spacecrime is not an act undertaken for other than financial motivations. Acts carried out for political or ideological ends that disrupt, damage, or destroy space assets of governments, civilians, or commercial entities are not spacecrime. These acts are distressing to the international community—analogous to incidents of late-twentieth century aircraft hijacking—but they are not spacecrime. Acts carried out for purely recreational or entertainment purposes are also not investigated. International responses to spacecrime should consider the potential for these actions, but they are not examined in this thesis.

Spacecrime is not undertaken by nation states against government, civilian, or commercial targets, even if the goal is financial gain. Space privateering is an intriguing concept: a nation-state employs a private individual or group to carry out an act of spacecrime on its behalf. There are further international ramifications should a nation state support a space-based act of aggression than if a private entity carried out the same act. For my purposes here, any act of space privateering is considered apart from the attribution of a nation-state supporter. In other words, whether the offender receives support from a nation-state or not is immaterial to my purposes—the intent here is to examine whether or not spacecrime, as defined above, will occur.

Spacecrime may include using cyber means to hijack and ransom a target satellite and/or its command and control (C2) system, but this type of spacecrime is cross-domain rather than a pure form. Hijacking and holding a satellite for ransom targets an on-orbit satellite from the ground, either by taking over the target's terrestrial C2 system, or using an offender's own C2 system to hack the satellite directly and wrest

---

[5] "TLS Customer Support Plan," *Transmitter Location Services LLC*, http://tlsglobal.com/CustomerSupportPlan.html.

control from its owner. Although such a scenario might be plausible, it is a separate act from spacecrime that occurs both in *and* from space. It is more properly understood as an act of *cybercrime* that targets assets *in* space, but *from* the earth. In this thesis I am primarily concerned with spacecrime actions that do not require direct interaction with a target satellite or its C2 system in order to achieve financial gain. If an offender were to utilize cyber means to hijack a satellite, and then use it to conduct an on-orbit attack against a different target, that act would compose spacecrime in this more pure form.

The following scenario provides a better illustration of the type of spacecrime investigated in this thesis. It is not necessary to examine every possible criminal vector to examine its practical and financial viability. I employ a maritime piracy model of hijacking and then ransoming a ship, albeit with some deviation based on the definition of spacecrime above. This example demonstrates how *one* scenario might play out in an act of future spacecrime. The discussion following the scenario unpacks the offender-target-guardian triad through examining the status of satellite technology and commercial space transportation options, the satellite market and availability of suitable targets, and the current state of guardianship in space.

One Possible Scenario

A small nanosatellite drifts toward a commercial satellite within the same orbital plane. The slow approach trajectory of the nanosatellite attracts the attention of space object and debris trackers. They attempt to contact the registered owner of the nanosatellite, only to find it is logged as nonoperational, and therefore categorized as debris. They notify the commercial satellite owner of the potential for collision. However, before the nanosatellite breaks the threshold for the commercial satellite operator to attempt a collision-avoidance maneuver, it slows its trajectory and stops its approach. When this new position

stabilizes, the company decides to simply monitor the object in collaboration with debris trackers, and continues with normal business.

After several months pass, the nanosatellite begins broadcasting noise on the uplink frequency of the commercial spacecraft, effectively jamming its target's ability to receive further commands from the ground. Due to the relatively close range of the nanosatellite, it requires only minimal power to successfully jam its target. During the next attempted contact with the commercial spacecraft, operators at the company realize they are unable to send commands or otherwise communicate with their satellite; they report the problem to their engineers and begin troubleshooting.

In parallel, the company leadership receives a ransom demand: unless the company pays the ransom, the offender will continue to hold the company's spacecraft hostage. At this point the company has no idea *how* its satellite is being jammed, or even *if* it is being jammed; all it knows is that it cannot command the satellite. Jamming from space is just one possibility among many, and not necessarily the most likely. The coincidental approach of the nanosatellite months ago does not register as a potential issue.

Without the ability to upload new commands, the company is at risk of being unable to fulfill its obligations to customer requirements. Although the satellite might have robust capabilities that allow safe operations for several days without commands from the ground, the company's business model requires regular commanding to meet customer needs.[6] Every lost opportunity in meeting customer needs represents lost revenue, and any delays in providing products to customers hurts its reputation.

---

[6] For example, remote sensing satellites must provide updated target sets in order for spacecraft to collect new data. This could be done several days or weeks in advance, but without daily contact the company could not meet short-notice customer needs.

The company's engineers determine there must be a source of interference, but have no idea from where it is originating. It could be a ground-based jammer, but such a system would only work while the satellite was directly overhead.[7] Since the inability to command persists across the entire low-earth orbit, this reason seems unlikely. They propose it might be a cybercrime attack, where the offender hacked the satellite directly and took control. However, their security architecture makes this very improbable; the offender would need the most current information regarding their proprietary hardware and software. The employees with access to such information are all employed within the company. If it were an insider threat, there is little they could do in the timeframe demanded by the ransom to avoid continued delays that affected revenue. If indeed an insider, they could investigate this possibility after the satellite was returned to full operational status.

After several days of various troubleshooting efforts, another demand from the offender arrives. It threatens to permanently damage or destroy the company's satellite if the ransom is not paid within 24 hours. The engineers are unable to assure leadership of the plausibility of the threat, but this new information indicates that jamming might be occurring *from* space. As far as they know, nobody has attacked a commercial satellite in this manner before, but they admit it is plausible. Without direct ties to their government, the company leaders are unsure of how to appeal to anyone in the international community for assistance. Even if they did, they believe the attacker would damage the satellite in response.

Without any other viable course of action, the company's top leaders relent and pay the ransom. They weigh the risks to revenue and reputation with their customers, and decide to keep the entire incident

[7] Unless the ground-based offender utilized system of jammers deployed worldwide to enable continuous interference.

confidential to avoid negative publicity and protect their stock prices. The offender confirms receipt of the funds, and the company regains control of its spacecraft. The nanosatellite remains dormant, lest it attract undue attention—the offender does not want to risk its identification as the source of jamming through the coincidence of its movement, and it retains the possibility of extracting additional ransom demands from this company after enough time passes. The total cost of the operation for the offender—nanosatellite construction, launch costs, ground equipment, personnel—was a fraction of the ransom received, leaving plenty of profit for future spacecrime endeavors.

While completely fictional, the scenario described above is possible with technology available in 2013. So why has this, or something like it, not yet occurred? The remainder of this chapter utilizes the three factors of Routine Activity Theory to examine the current and future status of offender, target, and guardianship in space. This analysis explains why spacecrime does not yet exist, and examines what near-term changes would allow such a scenario to come to pass. Although highly undesirable for all commercial spacefaring entities, it is unfortunately more plausible than at first glance.

Motivated and Capable Offender

A potential spacecrime offender must possess the technical skills to commit the criminal act and have access to a potential target. A robust military, civilian, and commercial space sector, combined with a growing educational and hobbyist segment, provides a significant community of individuals who possess the requisite knowledge and skills.[8] The technology required to create a satellite is easier to obtain and less costly than just a decade ago. Companies are making advances in small spacecraft technology at a rapid pace, promising increased

[8] Space Foundation, *The Space Report 2011*, 48.

capability, decreased size and weight, improved performance, and more modular spacecraft designs. It has never been cheaper or easier to build a satellite than in 2013. The prohibitive issue therefore is not the lack of capable offenders *per se*, but their current inability to operate *in* space.

Access to space is still accomplished via the pointy end of a well-controlled explosion—a rocket. From the Saturn V to the Space Shuttle to modern commercial launch vehicles, rocket technology has not evolved as much as that of its payloads. While some government programs exist for educational institutions to launch small research satellites for low or no cost, the nature of these programs make it difficult for a non-educational offender to take advantage of them.[9] Commercial launch providers continue to reduce overall costs and, in efforts to maximize profit per launch, they are creating more opportunities for small satellites as secondary payloads.[10] Over time these efforts will reduce the barrier of cost for space access.

The remainder of this section surveys the current status and projected near-term advances in small satellite technology. It examines existing and projected launch opportunities for the next decade, and provides launch costs for a notional offender nanosatellite over that timeframe. As satellite technology continues to evolve, and launch costs become more accessible, a supply of motivated individuals and groups will evolve with the means and access required to commit spacecrime.

Satellite Technology and Offender Capability

The future trend for satellite technology is similar to most modern electronic systems: smaller size, lighter weight, better performance, and

---

[9] "NASA - Educational Launch of Nanosatellites (ELaNa)," http://www.nasa.gov/mission_pages/smallsats/elana/.

[10] S. Wiens and K. Epstein, "Low Cost Deployment of Auxiliary Payloads," in *2000 IEEE Aerospace Conference Proceedings*, vol. 4, 2000, 329–334.

all at a lower cost.[11] The most effective entry point for a potential offender is not through traditional large-scale and long-duration spacecraft. These systems generally require specialized knowledge, contain highly complex and proprietary subsystems and hazardous materials, and demand high-cost components to achieve long on-orbit duration. In addition, since a proportionally lower number of people possess the capability to produce these systems, choosing such a path would aid in attribution by lowering the pool of potential suspects.

On the other hand, nano- or picosatellites offer the required capabilities in a low volume, low mass, single-purpose, modular, and relatively inexpensive package. *Nanosatellites* refer to those satellites with a total mass between 1.0 and 10 kilograms, while *picosatellites* are those with a total mass between 0.1 and 1.0 kilograms.[12] Several educational initiatives exist to encourage development of satellites using these smaller form factors.[13]

One of the most prominent emerging standards is the CubeSat Project, an open-source collaboration of over 40 educational and private institutions.[14] The CubeSat Standard, a specification created jointly by California Polytechnic State University and Stanford University, defines a one unit (1U) satellite as a cube of 10 centimeters per side, with maximum mass of 1.33 kilograms.[15] The specification allows for cubesats up to three units (3U) tall, as if each unit were a building block

---

[11] Howard E. McCurdy, *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program* (Baltimore, MD:The Johns Hopkins University Press, 2003).

[12] Surrey Satellite Technology, *Small Satellite Home Page*, http://centaur.sstl.co.uk/SSHP/sshp_classify.html

[13] Filippo Graziani, International Academy of Astronautics, "2nd IAA Conference on University Satellites Missions and the 2nd Cubesat Winter Workshop," http://iaaweb.org/content/view/524/695.

[14] CubeSat, "About Us," http://www.cubesat.org/index.php/about-us.

[15] CubeSat, *CubeSat Design Specification Rev 12*, 1 August 2009, http://www.cubesat.org/images/developers/cds_rev12.pdf.

stacked on top of each other.[16] The specification also allows for 6U and 12U configurations, although none have been launched as of 2012.[17] This standard led NASA to create the Poly-Picosatellite Orbital Deployer (PPOD), a standard launch platform for multiple cubesats. Using a PPOD adapter allows a launch provider to open its secondary payload capacity to any developer adhering to the specification, rather than needing to build proprietary adapters for each individual satellite.[18]

As cubesats become a standard for nanosatellite design, a drive towards modular and open, rather than proprietary, systems emerges. Since cubesats were born through the educational system, they have tended to include open hardware and software; designers often share their schematics and code with others freely. This helped breed a new generation of satellite integrators at the hobbyist and amateur levels (i.e. nonprofessional entities). For example, several individuals utilized Kickstarter, a popular crowdfunding site, to raise the capital necessary to build and launch nanosatellites.[19] For just over $110,000, one of the groups used the popular Arduino platform to build *and* launch two cubesats to carry out various on-orbit experiments for their financial backers.[20] Although these satellites do not contain the full capabilities required to carry out a spacecrime act as described in the scenario, it

---

[16] A 3U CubeSat would therefore be 10cm x 10cm x 30cm, with maximum mass of 4kg.

[17] Jessica Culler, "NASA Ames' E. Coli Small Satellite Study Selected for Flight," March 15, 2013, http://www.nasa.gov/centers/ames/news/2013/13-022AR-ecamsat-selection_prt.htm.

[18] National Aeronautics and Space Administration, *Launch Services Program, Program Level Poly-Picosatellite Orbital Deployer (PPOD) and CubeSat Requirements Document, LSP-REQ-317.01 Rev A*, http://www.nasa.gov/pdf/627972main_LSP-REQ-317_01A.pdf

[19] Alex Antunes, "The First Kickstarter Satellites," Sept 9, 2012, http://www.science20.com/satellite_diaries/first_kickstarter_satellites-93831.

[20] Peter Platzer, et al, "ArduSat - Your Arduino Satellite in Space," *Kickstarter*, http://www.kickstarter.com/projects/575960623/ardusat-your-arduino-experiment-in-space.

demonstrates a trend towards achieving the development and launch costs that will be attractive to potential offenders.

The significance of these initiatives comes in the drive to utilize hardware not specifically rated for use in space. Until recently, only space-qualified hardware and software were used in satellites; this resulted in generally outdated hardware with limited capabilities.[21] More recent hardware platforms such as Arduino, BeagleBone, Raspberry Pi and others provide satellite builders a wide variety of modular components to choose from, even if longevity on-orbit is less than their space-qualified alternatives.[22] The low cost and large user community for these systems makes them ideal for cubesats whose life expectancy might be measured in months rather than years.

The drive toward off-the-shelf satellite design is epitomized in recent efforts to use a commercial smartphone as the primary computer for a satellite. NASA successfully integrated and tested a smartphone-powered cubesat, and plans to launch its PhoneSat 2.0 in mid-2013.[23] Surrey Satellite Technology launched its STRaND-1 phone-powered cubesat in February 2013, effectively achieving the most powerful computer ever on-orbit.[24] As of May 2013, testing was ongoing to determine its performance and life span while in space. Cheap and powerful computational hardware, combined with readily available

---

[21] Miriam Krame, "PhoneSats in Space: Tiny NASA Satellites Have Smartphone Brains," April 23, 2013, http://www.space.com/20772-nasa-phonesats-smartphone-satellites.html.

[22] "Citizens in Space," http://www.citizensinspace.org; Arduino platform, http://www.arduino.cc; Beaglebone platform, http://www.beagleboard.org; Raspberry Pi platform, http://www.raspberrypi.org.

[23] Tricia Talbert, "PhoneSat: Smart, Small and Sassy," Dec 21, 2012, http://www.nasa.gov/offices/oct/home/PhoneSat.html

[24] Surrey Satellite Technology Limited, "World's first 'phonesat', STRaND-1, successfully launched into orbit," Feb 25, 2013, http://www.sstl.co.uk/News-and-Events?story=2123.

software development tools, promise to increase the capabilities of future satellite builders.

The benefits of standardized platforms for a future spacecrime offender are numerous. Building the satellite becomes easier with modular hardware components, open source software, and a large community of educational and hobbyist enthusiasts.[25] Solving tough challenges in development is a matter of crowdsourcing the problem under the guise of a legitimate experiment.[26] Obtaining launch access becomes less complex due to standardization of payload requirements from launch vendors—as long as the satellite fits in a provider's secondary payload bay, it has a way into space. The possibility of increased anonymity for an offender is also realized through using a standard platform. Since the offender's satellite looks just like hundreds of other cubesats on the outside, it might be difficult to distinguish its nefarious purposes from the experimental ones of its neighbor. The more cubesats are launched, the more difficult attribution becomes, and it increases the probability for the offender avoiding detection and/or identification.

Besides technological capability, offenders also need the requisite skills to design and build systems for the space domain. The complexities of orbital mechanics, electronics, physics, propulsion, thermodynamics, wireless communications, and the other fields comprising astronautics are not tamed simply through modular components, standardization, and open systems. Although these skills are certainly obtainable through self-study, analogous to how many individuals learn advanced computer skills, due to the complex interdisciplinary nature of the knowledge needed it is more likely an

---

[25] Song Hojun, "DIY Satellite," *Open Source Satellite Initiative*, http://opensat.cc/download/DIYSatellite_en.pdf

[26] Jeff Foust, "Crowdfunding Space," *The Space Review,* April 15, 2013, http://www.thespacereview.com/article/2279/1

offender would obtain these skills through formal education. In 2011 there were close to 18,909 students in the U.S. pursuing undergraduate aerospace engineering degrees. A total of 3,459 aerospace engineering students graduated that year—the highest total in a decade—out of 83,001 engineering graduates.[27] With 50-70 cubesats planned for launch in 2013 by US educational institutions, in addition to other small satellite programs, many of these students will have hands-on satellite design experience upon graduation.[28] With 2012 unemployment rates for engineers at less than two percent, the vast majority of graduates work in various aerospace industries.[29] Over 81,000 aerospace engineers work in the United States alone.[30] As students and professionals transfer their knowledge into the growing hobbyist community, the combination of technological osmosis with the growth of modular components will empower those without advanced degrees to engage in satellite development.

Lest one remain unconvinced that building satellites is within the grasp of those not working within the satellite industry, a book designed for teachers to help sixth graders (11-12 years old) build their own picosatellite debuted in 2010.[31] High school students have designed and

---

[27] Brian L. Yoder, "Engineering by the Numbers" in *Profiles of Engineering and Engineering Technology Colleges,* American Society for Engineering Education, 2011, http://www.asee.org/papers-and-publications/publications/college-profiles/2011-profile-engineering-statistics.pdf.

[28] Jeff Foust, "CubeSats Get Big," *The Space Review*, Sept 10, 2012, http://www.thespacereview.com/article/2155/1

[29] Christopher J. Gearon, "You're an Engineer? You're Hired," *US News and World Report*, March 22, 2012, http://www.usnews.com/education/ best-graduate-schools/articles/2012/03/22/youre-an-engineer-youre-hired.

[30] US Department of Labor, Bureau of Labor Statistics, "Aerospace Engineers: Occupational Employment and Wages, May 2012", http://www.bls.gov/oes/current/oes172011.htm

[31] Michael Paluszek, Eloisa de Castro, and Derrek Hyland, *The CubeSat Book*, (Plainsboro, NJ: Princeton Satellite Systems, Inc.), 2010.

built cubesats with launch services provided by NASA.[32] A series of do-it-yourself (DIY) books on satellite construction and the orbital environment were released by O'Reilly Media, a respected publisher of technical computer manuals.[33] The Space Foundation's *Space Report 2011* concluded, "construction of a cubesat is well within the reach of hobbyists and students."[34] Several successful crowdfunded satellite ventures are in development, while many other individuals work in "hacker spaces" across the country on their own projects.[35]

The point is not that these systems are capable of (or necessarily leading to) carrying out spacecrime *now*, but that the foundational knowledge, technological capability, and support infrastructure is in place. These hobbyists generally lead open-source initiatives, which could lead to further commoditization and modularization of space systems, similar to the Arduino platform's success in doing the same for the DIY electronics sector.[36]

Technology and capability in small satellite development have improved greatly over the past decade, and promise to evolve further. Many knowledgeable people exist and are already building and launching small satellites, from high school to university, hobbyist to professional.[37] This talent pool will increase as the technology becomes more accessible,

---

[32] Michael Seo, "NASA to Launch the First Satellites Built by High School Students," *Popular Mechanics*, March 22, 2011, http://www.popularmechanics.com/science/space/nasa/nasa-to-launch-the-first-satellites-built-by-high-school-students?click=main_sr; Thomas Jefferson High School CubeSat Program, "Systems Engineering at TJHSST," http://tj3sat.wikidot.com

[33] "Sandy Antunes, O'Reilly Media," http://www.oreillynet.com/pub/au/4997

[34] Space Foundation, *The Space Report 2011*, 4.

[35] Jeff Foust, "Hacking space," *The Space Review*, April 23, 2012, http://www.thespacereview.com/article/2068/1

[36] David Kushner, "The Making of Arduino," *Institute of Electrical and Electronics Engineers Spectrum*, Oct 2011, http://spectrum.ieee.org/geek-life/hands-on/the-making-of-arduino

[37] Giovanni Verlini, "The Bright Future of Small Satellite Technology," http://www.satellitetoday.com/via/features/The-Bright-Future-of-Small-Satellite-Technology_37150.html

modular, and open. The real challenge for potential criminals is therefore not the construction of a satellite capable of committing spacecrime, but getting that satellite into space. The following section addresses this challenge.

Launch Opportunities and Offender Access to Space

Access to space still occurs using essentially the same technology that launched Sputnik in 1957. Rocket science has not experienced many technological breakthroughs in the past five decades, with liquid hydrogen and liquid oxygen retaining their primacy.[38] Rocket engineering has indeed improved the efficiency of these rockets, but the average cost for launch in 2002 remained close to $12,000 per pound.[39] Small satellite initiatives have led to many opportunities for secondary payloads launches, but non-educational efforts still require per launch costs in excess of $60,000.[40] However, the international commercial launch market has reached a point where increased privatization and competition should begin driving down these costs. The increased supply of small satellite initiatives, combined with efforts to maximize profits for every launch, will create more and cheaper launch opportunities.[41] This lowers the cost barrier for space access, and gives potential spacecrime offenders the ability to operate in the space domain.

There are approximately 21 launch vehicles available for commercial use worldwide, ranging from a maximum capacity of 27-53,000 kilograms per launch to LEO, and 517-12,980 kilograms per

---

[38] Virginia P. Dawson and Mark D. Bowles, *Taming Liquid Hydrogen: The Centaur Upper Stage Rocket 1958-2002*, National Aeronautics and Space Administration, NASA SP-2004-4230, 2004, 4.

[39] Futron Corporation, *Space Transportation Costs: Trends in Price Per Pound to Orbit 1990-2000*, Sept 6, 2002, 6, http://www.futron.com/upload/wysiwyg/Resources/Whitepapers/Space_Transportation_Costs_Trends_0902.pdf.

[40] "What is your price?" http://nanoracks.com/resources/faq

[41] Alex Soojung-Kim Pang and Bob Twiggs. "Citizen Satellites: Sending Experiments into Orbit Affordably," Feb 9, 2011, http://www.scientificamerican.com/article.cfm?id=citizen-satellites

launch to GEO.[42] While there are currently no providers dedicated to launching microsatellites, most provide opportunities for auxiliary payloads for each launch.[43] For example, NASA coordinates launch opportunities for cubesats as auxiliary payloads on government launches; as of early 2012 eight have been launched, with a total of 55 selected for launch through 2014.[44] An Indian Space Research Organization (ISRO) launch carried six auxiliary satellites in addition to its primary payload, including one small satellite (74 kilograms), two microsatellites (14 kilograms each), and two cubesats (3.0 and 6.5 kilograms).[45] SpaceX provides cargo space aboard its Dragon capsule flights to the International Space Station (ISS) and, in partnership with NanoRacks, launches them directly from the ISS.[46] Some of the companies focused on suborbital space tourism are also looking for opportunities to insert small satellites into orbital trajectories during their flights.[47] As government, civilian, and commercial launch opportunities for auxiliary satellites increase, and standardization helps

---

[42] Federal Aviation Administration, *Commericial Space Transportation: 2011 Year in Review,* January 2012, 10-15; Space Exploration Technologies Corporation, "Falcon Heavy Overview," http://www.spacex.com/falcon_heavy.php.

[43] Matt Bille, Tom Hunsaker, and Paul Kolodziejski, "Nanosatellite Launch Vehicles: A Global Perspective and Business Case Analysis," presentation at the Rocky Mountain AIAA Technical Symposium, Oct 26, 2012, http://info.aiaa.org/Regions/MW/Rocky_MNT/ATS/ATS2012%20Presentations/Bille.pdf

[44] Joshua Buck, "NASA Announces Third Round Of CubeSat Space Mission Candidates," National Aeronautics and Space Administration, Public Release 12-050, Feb 14, 2012, http://www.nasa.gov/home/hqnews/2012/feb/HQ_12-050_CubeSats.html

[45] Indian Space Research Organization, "Commercial Payloads Launched by PSLV-C20," http://www.isro.org/pslv-c20/payloads.aspx

[46] "Smallsat Deployment," http://nanoracks.com/products/smallsat-deployment.

[47] Federal Aviation Administration, *The US Commercial Suborbital Industry: A Space Renaissance in the Making*, HQ-111460.INDD, 20-21, http://www.faa.gov/about/office_org/headquarters_offices/ast/media/111460.pdf.

commoditize the cubesat launch market, increased competition promises to decrease the price of launch.[48]

Some Russian launch providers currently launch cubesats as auxiliary payloads for approximately $40,000 per cube.[49] Launching with NanoRacks through its partnership with SpaceX and the ISS carries a price tag of $30,000 for educational and $60,000 for commercial users.[50] Other than obtaining a free ride through NASA's program, these represent the lowest launch cost available for commercial cubesats, with industry rates averaging approximately $85,000 per 1U cubesat. Future initiatives include not only expanded opportunities for launching cubesats as auxiliary payloads, but on dedicated nanosatellite launches as well. The Open Space Society announced its Small Cubesat Payload launch opportunity for 2015, promising to carry 50-100 cubesats in several size configurations into LEO aboard a single launch vehicle. As this initiative is part of its effort towards winning the Google Lunar X Prize, future missions could carry cubesats to GEO as well.[51]

Other than launch costs, access to space requires registration with the United Nations. Depending on the nation of registration, various national organizations may also require coordination, such as the Federal Communications Commission (FCC) and National Oceanic and Atmospheric Administration (NOAA) for radio frequency and earth observation approvals, respectively. Given the wide variety of launch options and locations, motivated criminals could find a way around paper registration requirements, either through fraudulent registrations

---

[48] Space News, "Small Satellite Launch Opportunities on the Rise," Aug 13, 2012, http://www.spacenews.com/article/small-satellite-launch-opportunities-rise.

[49] Jos Heyman, FOCUS: CubeSats - A Costing + Pricing Challenge," Oct 2009, http://www.satmagazine.com/cgi-bin/display_article.cgi?number=602922274

[50] "What is your price?" http://nanoracks.com/resources/faq

[51] Open Space Society, "Open Space Society Announces Capability for Commercial Payload Launch to Earth Orbit," Feb 28, 2013, http://www.teamfrednet.org/index.php?option=com_content&view=article&id=79

or other means. It could also be relatively simple to maintain anonymity, analogous to the registration process for commercial websites and the ineffectiveness of attribution based on that registration data alone. Regardless of these requirements, the continued success of transnational crime (or rather, the inability to eliminate it completely) demonstrates that no regulatory requirement is completely effective at eliminating crime and corruption.

Launch providers also impose security requirements to ensure obviously dangerous satellites are screened out, analogous to airport baggage and cargo screening. In most cases this would not detect satellites dedicated to spacecrime, since the hardware used for jamming another satellite resembles that used for innocuous purposes. Criminals prove themselves extremely resourceful in exploiting weaknesses in even the most thorough screening procedures.[52] But the threat of force is not necessary for successful spacecrime acts, and although some criminals might choose to employ the technology required for this, it is more likely the complexity and increased probability of detection prior to launch would dissuade most offenders.

A negative consequence of the growth of open hardware and software standards for satellites is that it raises the likelihood of exploitation and hijacking of space assets. Analogous to the hacker community in cyberspace, individuals will find weaknesses they can exploit within these systems. Whether hobbyist, educational, or even commercial satellites, any system that adheres to published standards assumes the risk that vulnerabilities could be discovered that allow unauthorized access or control. This could provide offenders an

[52] Several cases in recent years demonstrate this unfortunate truth: Yoram Schweitzer, "The Case of the 'Shoe Bomber': Lessons in Counter-terrorism—This Time at No Cost," International Policy Center for Counter-Terrorism, 2002, 4; ABC News, "Plot Would Have Killed Thousands," http://abcnews.go.com/WN/story?id=3451976; "Cargo Planes Bomb Plot," *Wikipedia, the Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Cargo_planes_bomb_plot.

alternative method to gain access to space, without the need to build and launch one's own satellite. If offenders can commandeer a satellite and use it for their purposes, they not only avoid development and launch costs, but also gain anonymity since the satellite remains registered to the party that launched it. It also greatly reduces the challenge of launching a satellite into a specific target orbit: an offender need only find a satellite that can be commandeered, and which possesses the capabilities necessary to carry out the jamming attack, in the same orbit as its target. Offenders are aided greatly by the owners of educational and hobbyist satellites, since both groups tend to publish detailed information about their systems on the Internet for the benefit of their respective communities.[53]

The purpose here is not to analyze the probability of this occurring, but merely to recognize that as modularization and commoditization of hardware, software, and knowledge increase, so do opportunities for offenders to exploit these efforts for nefarious purposes. Whether offenders build and launch their own satellites, or commandeer another's satellite to use for spacecrime purposes, the effect is the same—crime occurs both *in* and *from* the space domain. An offender could also take advantage of various vulnerabilities found in open-system satellite architectures to hijack a satellite directly from the ground, and then ransom it back to its owner. Although this would also amount to a form of spacecrime, and its probability is increased by using off-the-shelf hardware and software, this business case (and many others) is not considered here. This thesis focuses only on those acts that avoid direct, physical interaction with the target satellite itself (i.e. jamming) rather than those acts that affect the internal workings of the target (i.e. hacking).

[53] Tyler Moskowite, "Homemade Satellites are Just Around the Corner," *MAKE Magazine*, June 21, 2012, http://blog.makezine.com/2012/06/21/homemade-satellites-are-just-around-the-corner.

The primary challenge of space access in the near future is the relatively high cost, but these costs are within the reach of a well-funded offender, and promise to decrease over the next decade. An increased demand for small satellite launches, particularly via the cubesat standard, will drive commercial providers to provide a greater supply of launch opportunities. As new launch providers enter the market—from traditional large-scale companies such as SpaceX or Orbital Sciences to space tourism companies looking to maximize profit through launching a handful of cubesats—competition will most likely drive down the cost for auxiliary payload launches.[54] Cubesats hold the potential to commoditize nanosatellite launch options, since standardization of launch mechanisms benefits both satellite developers and launch providers.[55] As costs become less, one barrier to committing spacecrime is lowered. The next element in an offender's spacecrime cost/benefit calculus is the value of the target, the topic of the next section.

Supply of Suitable Targets

There are currently 1046 operational satellites in orbit around the earth, and approximately 460 of them are commercial satellites and potential targets for spacecrime.[56] This quantitative assessment is not sufficient to conclude all of these are suitable targets, and therefore a qualitative assessment is required. The suitability model from Chapter 1—value, inertia, visibility, and accessibility—is used in the following sections to analyze whether suitable targets exist in sufficient quantities to entice an offender into committing spacecrime. Each factor is examined in sufficient detail to conclude there are currently enough

[54] FAA, *The US Commercial Suborbital Industry,* 20-21.

[55] John Garvey, "The Innovator's Dilemma and the Emerging Market in CubeSat Launch Services," speech at AIAA Dinner Meeting, March 24, 2010.

[56] "UCS Satellite Database," *Union of Concerned Scientists*, http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html.

commercial satellites in orbit to permit spacecrime to occur. Growth in the commercial satellite market only serves to enlarge this supply of suitable targets.

Value

The value of a given satellite relates to the ability of an offender to exact remuneration from the target's owner. The amount of potential financial extraction correlates to the targeted satellite's significance in the owner's revenue stream. In other words, the targeted satellite must be worth enough to offenders to justify their required costs for extortion, and it must also be worth enough to its owner to justify paying a given ransom. The global commercial satellite market supports this concept of value.

According to a 2011 report, revenues for the global commercial space products and services sector were approximately $102 billion, an increase of nine percent over the previous year.[57] The direct-to-home television subsector led the industry with $79.2 billion, followed by satellite communications at $17.9 billion, satellite radio at $2.8 billion, and earth observation at $2.0 billion. Global revenues increased an average of 10.7 percent per year from 2001 to 2011, and growth in all sectors is expected to continue over the next decade.[58] Each subsector presents unique targets in a variety of orbits, and none is invulnerable to the scenario presented earlier.

Revenue is certainly an important aspect of value, but so is the cost of the satellite itself—commercial satellites are very expensive. The cost for individual satellites varies by mission: a modern commercial imaging satellite might cost $800 million, while a communications

---

[57] Space Foundation, *The Space Report 2011*. As stated earlier, the entire global space economy produced an estimated $189.4 billion in revenue, of which $102 billion came from the commercial space products and services sector.

[58] Satellite Industry Association, *2012 State of Satellite Industry Report*, May 21, 2012, 10, http://www.sia.org/wp-content/uploads/2012/05/FINAL-2012-State-of-Satellite-Industry-Report-20120522.pdf

satellite might cost $150-650 million.[59] Replacing a satellite not only requires the costly construction of a new satellite, but also the cost of launching the replacement, as well as the revenue foregone from the outage. Launch costs might be decreasing as described earlier, but optimistic estimates of $5000 per pound still results in a $20 million price tag for a 4000 pound LEO imaging satellite.[60] A communications satellite in GEO might weigh 13,000 pounds or more.[61] It appears the more fiscally responsible choice is to avoid the need to replace satellites already on orbit before exhausting their planned operational lives.

In one example of a satellite outage, XM Radio subscribers went without service for 24 hours in May 2007 due to technical difficulties with one of its geosynchronous satellites. The problem was due to internal causes, not from an external threat, but it still is a useful example for examining the financial repercussions of service interruptions. With over eight million subscribers at the time, had each requested a refund of a single day's service it would have cost the company almost $8 million in lost revenue.[62] Some subscribers claimed the company was negligent and within days initiated a class-action lawsuit. Fortunately for the company, it had already offered a one-dollar credit for any subscriber who requested it, and the case was dismissed just over a year later. Despite this legal success, and despite receiving

---

[59] Aerospace Technology, "GeoEye-2 Earth Observation Satellite, United States of America," http://www.aerospace-technology.com/projects/geoeye-2-satellite; Robert Charette, "High Costs of Satellites Impeding Future Communications?" *Institute of Electrical and Electronics Engineers Spectrum*, May 1, 2008, http://spectrum.ieee.org/riskfactor/computing/it/high_costs_of_satellites_imped.

[60] These are gross estimates; more costs comprise a launch than merely per pound estimates, to include insurance, registration, etc.

[61] "A Dual Launch for Global Communications," *Arianespace Launch Press Kit*, 7, http://www.arianespace.com/images/launch-kits/launch-kit-pdf-eng/VA208-INTELSAT-20-HYLAS-2-GB.pdf.

[62] David Lieberman and Laura Petrecca, "XM offers refunds after 24-hour outage is fixed," *USA Today,* May 22, 2007, http://usatoday30.usatoday.com/money/media/2007-05-22-xm-outages_N.htm.

fewer than $1000 in refund requests, the yearlong legal process was still very costly.[63] With over 20 million subscribers today following XM's merger with Sirius radio, this example demonstrates the real-world impact of interfering with commercial satellite services. An offender could exert tremendous leverage on such a company, and the alternatives to paying a ransom—losing a large amount of revenue, damaging company prestige, losing customers to a rival service, or getting involved a legal dispute—raise the probability that an offender might succeed in an extortion attempt.

Value is therefore a function of both the revenue a satellite generates, and the replacement cost of the satellite itself. Since an offender threatens to exact costs to a target satellite's owner in both these areas, it seems plausible that as long as a ransom was reasonable compared to the alternative, a company would choose to pay it. Without any ability to stop the offender's attack, the company appears to have little recourse.

Inertia

In the context of the space domain, inertia refers to the physical characteristics of a satellite as expressed by its orbit. The altitude of a satellite determines its velocity, and its inclination governs where on the earth's surface the satellite can be seen. The satellite's mission governs both, and therefore certain missions tend to require specific orbits. Space might seem infinite compared with the finite nature of terrestrial transportation options, but in practice the orbits of cislunar space are quite analogous to sea and air routes. This relative predictability helps restrict the challenges facing an offender in accessing a suitable target.

Commercial satellites are mostly located in low-earth orbit (LEO) or geosynchronous orbit (GEO), with roughly an equal number of targets in

---

[63] Jesse Greenspan, "XM Wins Dismissal Of Proposed Class Action," Sept 30, 2008, http://www.law360.com/articles/70986/xm-wins-dismissal-of-proposed-class-action.

each.[64] However, the variety of orbital altitudes, planes, and inclinations for LEO satellites makes access more challenging. Due to the small size and limited propulsion potential of cubesats, offenders would need to launch their satellites into as near an orbit to the target as physically possible. Whereas changing altitude should not pose insurmountable technical challenges, changing planes or inclination could prove impractical or impossible once on-orbit. The offender would either need to accept a launch opportunity into whatever orbit was available, attempt to find an opportunity to launch into the same orbit as the target, or obtain launch access as a secondary payload on the target satellite's booster. These are difficulties that can be overcome, but which could drive an offender towards different targets entirely.

A slightly smaller number of commercial GEO satellites present fewer target opportunities, but their assignment to a limited number of regulated positions makes targeting any one of them far easier. Should offenders choose a geosynchronous commercial target, they need only achieve geosynchronous orbit to greatly simplify their ability to rendezvous with a potential target.

Visibility

Visibility in space refers to the specific location of the satellite, similar to inertia but more specific. Whereas inertia relates to the predictability of satellite orbits due to physics, visibility relates to the ability of an offender to locate a specific target in space. The United States helpfully provides the location of all orbital objects, including commercial satellites, for free to the international community.[65] In addition, an international group of amateur satellite spotters compiles data using various means and publishes it for anyone to access.[66] If all

---

[64] SIA, *2012 State of Satellite Industry Report*, 6.

[65] Accessible through websites such as Space-Track (https://www.space-track.org).

[66] One such community is the Colorado Springs Astronomical Society's Earth Orbiting Satellite Observers Club (http://csastro.org/eosoc).

else fails, an offender could resort to intelligence gathering techniques to extract a target satellite's current location.[67] It is beyond the scope of this thesis to prove the technical ability to locate the orbital position of a target satellite, but the plethora of available data and analytic tools suggests they reduce the difficultly tremendously.

Given the pervasiveness of GPS technology, most modern satellites utilize satellite navigation signals to locate themselves on orbit. Although offenders won't necessarily have direct access to this information about a target, they will know their own location precisely. Since the offender need not traverse very close to a target to execute a jamming attack, the available data is sufficient to allow planning for rendezvous and proximity operations.

Accessibility

The ability to gain physical access to a target satellite is one aspect of spacecrime, but avoiding detection, attribution, and/or apprehension further guides an offender's cost/benefit analysis of a target's suitability. If the nature of a potential victim is such that targeting it would lead to undue attention and retaliation, an offender might choose another target without such consequences. For this reason, an offender would most likely avoid targeting satellites associated with any nation with the technical means to identify the source of on-orbit jamming or locate terrestrial command and control signals. For example, targeting an American military, civilian, or commercial satellite is likely to evoke a strong national response, as would targeting a satellite associated with a nation allied or partnered with the United States. However, selecting a private commercial satellite from a nation without close ties to a major space power is more prudent.

[67] Christopher Hadnagy, *Social Engineering: The Art of Human Hacking*, (Hoboken, NJ: Wiley, 2010).

There is no international governing body to respond to criminal acts in space. Because of this, any private company must appeal to its national government for help in responding to spacecrime threats. This nation state must then entreat the international community to assist. Even if a space power with the means to help agrees to do so, the process of obtaining its assistance takes time. When adding the difficulties in locating the source of jamming in space, attributing it to individuals or group owners, geolocating the offenders on earth, and finally tracking and apprehending them, the likelihood of accomplishing this before the private entity loses an inordinate amount of revenue is minimal—the target is more likely to pay the ransom when in this position of weakness rather than lose the ability to earn future revenue with the satellite. By the time the ransom is paid, the offender retains the initiative—if it is difficult to locate a source of jamming in space while the jamming is in progress, it is impossible to do so once the offender turns off the jamming signal. The offender's satellite returns to its status as just another small object in orbit, or, if the offender so chooses, could command it to reenter and burn up in the atmosphere (if located in LEO), thus removing all physical evidence of its existence.

Based on the factors of value, inertia, visibility, and accessibility, there are a sufficient number of suitable targets worthy of a potential offender's attention. The capabilities of a potential offender and the ability to access specific orbits restrict and help determine which targets are suitable for that particular offender; all offenders have their own decision calculus, and may thus arrive at different sets of suitable targets. Just as the offender-target interaction affects this analysis, so does the target-guardian relationship. The accessibility of the target, and therefore the ability of an offender to succeed in a spacecrime endeavor without apprehension, is directly related to the lack of capable guardianship in space. The following section discusses this relation and the current status of space guardianship.

Lack of Guardianship

Guardians serve to prevent crime through the primary mechanisms of observation and response. As discussed in Chapter 1, the presence or absence of capable guardians directly impacts the probability of criminal activity occurring. Guardianship in space involves finding, tracking, and identifying space objects through various technological means of observation. This could include permanently emplaced methods such as advanced radars or large optical telescopes, mobile terrestrial systems, and space-based systems. The United States Space Surveillance Network (SSN) is the most robust system currently in existence, but America does not hold a monopoly on terrestrial and space-based means of observation. Several countries and international organizations possess some means of space surveillance, and amateur satellite trackers have an active community dedicated to tracking objects in orbit.[68]

Applied to spacecrime, the task of finding, tracking, and identifying objects in space is not the most difficult aspect of observation. Every object launched into space is currently registered per the 1976 *Convention on Registration of Objects Launched into Outer Space* with the United Nations Office for Outer Space Affairs (UNOOSA).[69] The challenge comes in attributing interference or jamming to a specific object located *in* space. It is difficult enough to geolocate terrestrial sources of satellite jamming, but when the *geo-* is not part of the *location,* the problem becomes significantly more complex. In the earlier scenario, the coincidence of approach of the pirate satellite to the target would likely help *logically* determine the source of on-orbit jamming. However, the problem of proving it with certainty is *technical*, and therefore presents

---

[68] Brian Weeden, "Space Situational Awareness Fact Sheet," *Secure World Foundation*, Feb 1, 2012, http://swfound.org/media/1800/ssa%20fact%20sheet.pdf

[69] "Registration of Objects Launched into Outer Space," United Nations Office of Outer Space Affairs, http://www.unoosa.org/oosa/en/SORegister/index.html.

legal problems—if it is not possible to attribute blame to an on-orbit offender with assurance, the owner of the satellite could merely dispute or claim ignorance of any charges of wrongdoing.

If attribution to a specific object were possible, the next step would be to identify and find the physical location of the offender on earth. Spacecrime might occur *in* and *from* space, but for now the criminals must still live and operate on land or sea. The problem of locating a continuous ground-to-space jamming source is complex, but relatively straightforward.[70] The offenders are usually located near the jamming equipment, so once the source of jamming is located, so are the offenders.

With a jamming source located in space, offenders could be located anywhere on earth within view of their satellite. The nature of on-orbit operations and modern satellite on-board processing reduces the need to be in continuous contact. Offenders need only transmit upload commands to maneuver into position, toggle power for the jamming signal, or otherwise change the satellite's state in some way. Once in position and engaged in the spacecrime act, little to no communication with the satellite is required. The technical complexities of quickly locating these intermittent transmitters are immense, as evidenced by the proliferation of low-power cell phone and GPS jammers and the ineffectiveness of detection and enforcement to date.[71] If a guardian cannot locate the offenders, it becomes difficult to take action against them.

---

[70] David Patrick Haworth, "Locating the Source of an Unknown Signal," US Patent 6 018 312, Jan 25, 2000; Gerard A. Desjardins, "TDOA/FDOA Technique for Locating a Transmitter," US Patent 5 570 099, Oct 29, 1996. See also http://www.integ-europe.com/products/satellite-interference-geolocation, http://www.sat.com/products/satID.php, and http://en.wikipedia.org/wiki/Satellite_geolocation.

[71] "No Jam Tomorrow," *The Economist*, Q1:2011, http://www.economist.com/node/18304246.

Even if a guardian is able to find, track, identify, and attribute the source of an attack, a guardian must also be able to *act* to deter crime. The presence of a security guard might deter a shoplifter, but if the guard is forbidden from leaving the store, the thief is more likely to commit the crime and risk a chase, knowing the pursuit will be brief and escape more certain. Terrestrial examples of interference with space assets to date primarily involve nation-state actors, but the challenge would be at least as difficult for non-state actors and private corporations.[72]

Even with perfect intelligence and attribution of malfeasance, there are few mechanisms in place to take action against an offending asset located in space. While indirect action is possible—diplomatic pressure, terrestrial and transnational investigation and law enforcement, etc—those activities are not the focus of this thesis. Routine Activity Theory suggests a guardian needs to converge in *space and time* with an offender to be effective. Just as there are indirect methods to deal with piracy at sea, guardianship deals with the ability to respond directly to the threat *in its domain*. An aircraft might present a threat to a pirate mothership, but once the pirates hijack a vessel, any direct response must come from the sea. Without the ability to interdict, board, inspect, and commandeer, the only alternative is to sink the vessel—a decidedly suboptimal choice. This suggests true guardianship in space requires not only the ability to passively observe the space domain, but also to take direct action *in space*. There are many potential ways to address this requirement, but such speculation is left for further research.

The point here is that without adequate guardianship, the only way to deter spacecrime is through manipulating the other two factors: offenders and targets. For any other category of crime, it would be

[72] Monte Morin and Joel Rubin, "Cuba Jams Broadcasts to Iran, U.S. Says," *The Los Angeles Times*, July 17, 2003, http://articles.latimes.com/2003/jul/17/local/me-irantv17.

unthinkable for leaders and policymakers to disregard an entire assortment of deterrence mechanisms because of political sensitivities. The next chapter summarizes the application of Routine Activity Theory to the space domain, and then offers some concluding thoughts on how policymakers might employ these ideas in the future.

CHAPTER 3

Conclusion and Application

Society prepares the crime, the criminal commits it.

Henry Thomas Buckle

You ever get the feeling all hell's about to break loose and there's nothing you can do about it?

Ali Vali
The Devil Unleashed

The convergence in space and time of offenders and targets, in the absence of capable guardianship, is closer in 2013 than at any other point in history. Since companies are reluctant to disclose crime publicly for fear of economic consequence and loss of consumer confidence, it is possible such an attack has already occurred.[1] Technological progress will make building and operating small satellites cheaper and easier, while providing continually increasing levels of satellite performance. Combined with the decreasing cost for access to space through the commercialization of launch services, the number of potential offenders will continue to grow over the next decade.[2] A wide variety of suitable targets exist today, and the commercial space sector is expected to continue growing.[3] No single nation or organization has the capacity currently to exercise guardianship over space. With looming fiscal constraints facing the United States, it is unlikely to expand or acquire the required terrestrial and orbital systems necessary to observe, attribute, and act on criminal threats in space. Routine Activity Theory

---

[1] Nicole Perlroth, "Some Victims of Online Hacking Edge Into the Light," *The New York Times*, Feb 20, 2013, http://www.nytimes.com/2013/02/21/technology/hacking-victims-edge-into-light.html.

[2] As noted in Chapter 1, when the pool of capable offenders is large enough, at least some of them will become motivated to commit criminal acts. The actual motivations will be as varied as the individual criminal techniques employed.

[3] Federal Aviation Administration, *2012 Commercial Space Transportation Forecasts,* FAA Commercial Space Transportation Advisory Committee, May 2012.

predicts this nexus of offender-target-guardian characteristics provides the necessary conditions for spacecrime to occur.

Besides its utility in predicting the rise of spacecrime, Routine Activity Theory also provides value in determining what actions might help deter such crime. Manipulating any of the three factors has an influence on the amount of crime, and the current lack of offenders provides some evidence of this: no offender, no crime. The same is true for a lack of targets or achievement of perfect guardianship: either condition would result in zero crime. The challenge is that none of the factors can be manipulated into its ideal state without substantial costs.[4] Therefore policymakers must analyze each factor individually, and decide how to optimize resources in an effort to prevent as much crime as possible. The following sections present some possible options to address each of the factors.

Reducing offenders in space will continue to center around the issue of *access*. If the ability to access space can be controlled, then the number of offenders operating there can be reduced. Physical access can be regulated by individual nations, by launch providers, and by international regulating organizations. By increasing the difficulty of gaining access to space, governments and launch companies can manipulate the number of potential offenders. The potential still exists for offenders to utilize cyber and other means to take control of satellites already on-orbit, but this is also an issue of access. A company controls the ease or difficulty of this potential through its choice of hardware, software, and associated security technologies for its satellite systems. As companies move towards modular and open-source hardware and software, these attempts to reduce cost and increase efficiency must be

[4] For example, London's pervasive closed-circuit camera surveillance represents a well-funded attempt at achieving localized, near-perfect passive guardianship, but has had arguably little effect on crime rates. For more information see Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV,* UK Home Office Research Study 292 (Feb 2005).

balanced against security and the risk of criminal activity. By ensuring robust security architectures of its systems, the company can reduce the potential for manipulation, and therefore control access.

The suitability of a target satellite rests primarily on its value and accessibility—can an offender extract monetary value from the target and get away without being apprehended? Although the *number* of potential targets is likely to continue to increase over the next decade, their *suitability* can still be manipulated. In the context of the scenario presented earlier in this chapter, the value of a target rests in a company's willingness to pay a ransom rather than lose revenue, prestige, or the satellite itself. An insurance regime could be created that would cover the costs of lost revenue and replace a lost satellite, allowing a company to refuse to pay the ransom without financial impact. As more companies acquired this insurance, the viability of spacecrime of this type would diminish greatly—if a target is unwilling to pay, and incurs little penalty by doing so, then an offender has little recourse but to continue jamming its target (with no financial result), move on to a more suitable target (admitting defeat), or follow through with its threat and destroy the target (eliminating its on-orbit asset). The first option is effective if the target incurs costs exceeding the ransom requested, but effective insurance negates the offender's leverage. The last option makes little sense, as it would destroy the offender's investment completely. The offender would most likely find a more suitable target. However, if a majority of companies joined the insurance regime, the list of suitable targets would be short, and the physics of orbital mechanics would restrict the list further. The offender might choose to target a noncommercial actor, but then risks escalating the response from a private entity to one with closer ties to a nation state. This further reduces the target's suitability by increasing the likelihood of apprehension. An insurance regime might suffer from collective action issues that decrease its effectiveness and make it an imperfect response,

but is just one potential response among many possibilities for consideration.[5]

Assuming offenders are able to access space and find suitable targets, increased guardianship can affect the cost/benefit calculation of potential criminals and reduce their motivation to attempt spacecrime. Guardianship in space consists of observation, attribution, and action. Improved technical means to observe objects satellite *from* space, both visually and electronically, would contribute to reducing the ability of an offender to commit spacecrime undetected and unattributed. But attribution in space does not mean attribution on the earth, and laws are only enforced and arrests only made on land or sea. In the given scenario, it would be near-impossible to geolocate offenders who requires only a few minutes to command their satellite each day, require relatively low power to do so, and can accomplish it from any location around the globe. Geolocating an offender on earth would require capabilities beyond those currently available in space.

I did not examine the back-end requirements of spacecrime in this thesis: collecting the ransom, laundering the money so it can be used for legitimate purposes, and doing it all while remaining anonymous and alluding authorities. Since these necessary activities are comparable to those required for other transnational crime—drugs, human trafficking, maritime piracy, cybercrime, etc—and since those crimes have not been eliminated, spacecrime offenders should be able to execute their business model without additional effort beyond what other transnational criminals must do.

In order to exercise effective guardianship *of* space, there must exist means to take action *in* space. A variety of options are possible for responses to space threats, including but not limited to: defenses for

[5] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*, (Cambridge, MA: Harvard University Press, 1971).

targeted satellites (either within the satellite itself, or separate satellites that act as bodyguards), ground-based options such as lasers or orbital interceptors, or on-orbit active response measures (not part of the target satellite system). These options are all expensive, technically complex, rife with politically sensitive challenges, and worthy of further examination by others. When spacecrime occurs and a targeted satellite owner implores its government to do *something*, unless guardianship is improved, there might be no option other than to pay the ransom, thereby encouraging more attacks. Crime flourishes in the absence of effective guardianship.

Ultimately, the decision on how to balance responses to these three factors rests with policymakers. For example, America decided having planes hijacked or used as weapons was such an abhorrent possibility that it responded physically and financially in all three areas. Offenders were reduced through additional scrutiny at flight training schools. Targets are made less suitable by reinforcing cabin doors, making them more difficult to hijack. Guardianship was increased through airport screening of passengers and cargo, restrictions on what may be carried aboard an aircraft, installing air marshals to instill uncertainty, and other methods. In addition, the US improved its overall intelligence, surveillance, and reconnaissance methods, and works much more closely with the international community to find and defeat potential offenders before they can take action. These efforts exert tremendous influence upon a potential offender's cost/benefit analysis, and therefore reduce (but do not eliminate) threats to aircraft.

Without lives on the line, it is unlikely such a response would occur to protect machines operating in space. However, the number of commercial initiatives in manned space tourism and exploration are

increasing.[6] It appears that private astronauts are moving from the realm of science fiction into reality.[7] When manned platforms become potential targets, the decision calculus changes considerably—without an effective way to respond to threats, ransoms are even more likely to be paid. The simple framework of offender-target-guardian therefore provides a robust model for not only predicting that spacecrime will occur, but for deciding what actions to take to mitigate the threat *before* it becomes reality. The future is not determined for humanity—it determines its future through the decisions it makes and the actions it chooses to take today.

When the first offender decides to commit crime in space, *someone* must do something about it. The international community may take a strong stance analogous to maritime piracy: the cost to do nothing is too high and only encourages more piracy, so it became a global problem that garnered an international response. While spacecrime could exact large costs in prevention attempts, it could also provide benefits to society at large. Just like the global cybersecurity industry, spacecrime might drive new research and development agendas, lead to new technologies, and result in new jobs centered on protection of space assets and spacecrime prevention. Economists might argue that spacecrime would benefit society in the aggregate, especially since no humans are yet physically affected by the criminal act. There might be more wealth created from a small amount of crime in space than if spacecrime were never to ever arise, but this line of argument is well beyond the scope of this thesis. Policy makers and economists must examine these and other issues in future research.

---

[6] Federal Aviation Administration, *The US Commercial Suborbital Industry: A Space Renaissance in the Making*, HQ-111460.INDD, 20-21, http://www.faa.gov/about/office_org/headquarters_offices/ast/media/111460.pdf.

[7] "SpaceX to Launch Private Astronauts in 2015," *Space Industry News*, http://spaceindustrynews.com/spacex-to-launch-private-astronauts-in-2015/2221/.

BIBLIOGRAPHY

Academic Papers

Becker, Gary S. "Crime and Punishment: An Economic Approach." Journal of Political Economy 76, no. 2 (January 1968).

Bennett, Richard R. "Routine Activities: A Cross-National Assessment of a Criminological Perspective." Social Forces 70, no. 1 (September 1, 1991): 147–163. doi:10.1093/sf/70.1.147.

Buck, Joshua. "NASA Announces Third Round Of CubeSat Space Mission Candidates." National Aeronautics and Space Administration Public Release 12-050. Feb 14, 2012. http://www.nasa.gov/home/hqnews/2012/feb/HQ_12-050_CubeSats.html

Clarke, Ronald V., and David Weisburd. "On the Distribution of Deviance." In *Policy and Theory in Criminal Justice: Contributions in Honour of Leslie T. Wilkins*, by Don Gottfresdon (Aldershot, UK: Avebury, 1991).

Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (August 1979): 588.

Cohen, Lawrence E., Marcus Felson, and Kenneth C. Land. "Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977." *American Journal of Sociology* 86, no. 1 (July 1980): 90.

Eck, John E. "Drug Markets and Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing." Doctoral Dissertation, University of Maryland, 1994.

McCarthy, Bill. "New Economics of Sociological Criminology." Annual Review of Sociology 28, no. 1 (August 2002): 417–442.

Pratt, Travis C., Kristy Holtfreter, and Michael D. Reisig. "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." Journal of Research in Crime and Delinquency 47, no. 3 (August 1, 2010): 267–296.

Selva, Daniel, and David Krejci. "A Survey and Assessment of the Capabilities of Cubesats for Earth Observation." Acta Astronautica 74 (May 2012): 50–68.

Tauchen, Helen. "Estimating the Supply of Crime: Recent Advances," in Handbook on the Economics of Crime, by Bruce L Benson and Paul R Zimmerman (Northampton, MA: Edward Elgar, 2010).

Tseloni, Andromachi, Karin Wittebrood, Graham Farrell, and Ken Pease. "Burglary Victimization in England and Wales, the United States and the Netherlands A Cross-National Comparative Test of Routine Activities and Lifestyle Theories." British Journal of Criminology 44, no. 1 (January 1, 2004): 66–91.

Winton, Harold R. "An Imperfect Jewel: Military Theory and the Military Profession." Journal of Strategic Studies 34, no. 6 (2011): 853–877.

Yar, Majid. “The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory.” European Journal of Criminology 2, no. 4 (October 1, 2005): 407–427.

Articles

"A Dual Launch for Global Communications." Arianespace Launch Press Kit. http://www.arianespace.com/images/launch-kits/launch-kit-pdf-eng/VA208-INTELSAT-20-HYLAS-2-GB.pdf.

Antunes, Alex. "The First Kickstarter Satellites." Sept 9, 2012. http://www.science20.com/satellite_diaries/first_kickstarter_satellites-93831.

Bouwmeester, J., and J. Guo. “Survey of Worldwide Pico- and Nanosatellite Missions, Distributions and Subsystem Technology.” Acta Astronautica 67, no. 7–8 (October 2010): 854–862.

Charette, Robert. "High Costs of Satellites Impeding Future Communications?" *Institute of Electrical and Electronics Engineers Spectrum*. May 1, 2008. http://spectrum.ieee.org/ riskfactor/computing/it/high_costs_of_satellites_imped."Citizens in Space," http://www.citizensinspace.org.

CubeSat, "About Us," http://www.cubesat.org/index.php/about-us.

Culler, Jessica. “NASA Ames’ E. Coli Small Satellite Study Selected for Flight.” March 15, 2013. http://www.nasa.gov/centers/ames/ news/2013/13-022AR-ecamsat-selection_prt.htm.

Desjardins, Gerard A. “TDOA/FDOA Technique for Locating a Transmitter,” US Patent 5 570 099 (Oct 29, 1996).

"Details of Telstar-1," *United States Space Objects Registry*. http://usspaceobjectsregistry.state.gov/registry/dsp_DetailView.cfm?id=90

Foust, Jeff. "Crowdfunding Space." *The Space Review*. April 15, 2013. http://www.thespacereview.com/article/2279/1

———, "CubeSats Get Big," *The Space Review*. Sept 10, 2012. http://www.thespacereview.com/article/2155/1

———. "Hacking space." *The Space Review*. April 23, 2012. http://www.thespacereview.com/article/2068/1

Gearon, Christopher J. "You're an Engineer? You're Hired." *US News and World Report*. March 22, 2012. http://www.usnews.com/education/best-graduate-schools/articles/2012/03/22/youre-an-engineer-youre-hired.

"GeoEye-2 Earth Observation Satellite, United States of America." *Aerospace Technology*. http://www.aerospace-technology.com/projects/geoeye-2-satellite.

Greenspan, Jesse. "XM Wins Dismissal Of Proposed Class Action." Sept 30, 2008. http://www.law360.com/articles/70986/xm-wins-dismissal-of-proposed-class-action.

Haworth, David Patrick. “Locating the Source of an Unknown Signal.” US Patent 6 018 312 (Jan 25, 2000).
Heyman, Jos. "FOCUS: CubeSats - A Costing + Pricing Challenge." Oct 2009. http://www.satmagazine.com/cgi-bin/display_article.cgi?number=602922274
Hojun, Song. "DIY Satellite." Open Source Satellite Initiative. http://opensat.cc/download/DIYSatellite_en.pdf
Indian Space Research Organization. "Commercial Payloads Launched by PSLV-C20." http://www.isro.org/pslv-c20/payloads.aspx.
Kigerl, Alex. “Routine Activity Theory and the Determinants of High Cybercrime Countries.” Social Science Computer Review 30, no. 4 (November 1, 2012): 470–486.
Krame, Miriam. "PhoneSats in Space: Tiny NASA Satellites Have Smartphone Brains," April 23, 2013, http://www.space.com/20772-nasa-phonesats-smartphone-satellites.html.
Kushner, David. "The Making of Arduino." *Institute of Electrical and Electronics Engineers Spectrum*, Oct 2011. http://spectrum.ieee.org /geek-life/hands-on/the-making-of-arduino
Lieberman, David, and Laura Petrecca. "XM offers refunds after 24-hour outage is fixed." *USA Today*. May 22, 2007. http://usatoday30.usatoday.com/money/media/2007-05-22-xm-outages_N.htm.
Morin, Monte, and Joel Rubin. "Cuba Jams Broadcasts to Iran, U.S. Says." *The Los Angeles Times*. July 17, 2003. http://articles.latimes.com/2003/jul/17/local/me-irantv17.
Moskowite, Tyler. "Homemade Satellites are Just Around the Corner." *MAKE Magazine*, June 21, 2012 http://blog.makezine.com/2012/06/21/homemade-satellites-are-just-around-the-corner.
“NASA - Educational Launch of Nanosatellites (ELaNa).” Accessed May 5, 2013. http://www.nasa.gov/mission_pages/smallsats/elana/.
“No Jam Tomorrow.” The Economist, 2011, Q1 edition. http://www.economist.com/node/18304246.
"Open Space Society Announces Capability for Commercial Payload Launch to Earth Orbit." *Open Space Society*. Feb 28, 2013. http://www.teamfrednet.org/index.php?option=com_content&view=article&id=79
Pang, Alex Soojung-Kim, and Bob Twiggs. "Citizen Satellites: Sending Experiments into Orbit Affordably." Feb 9, 2011. http://www.scientificamerican.com/article.cfm?id= citizen-satellites
Perlroth, Nicole. "Some Victims of Online Hacking Edge Into the Light." *The New York Times*. Feb 20, 2013. http://www.nytimes.com/2013/02/21/technology/hacking-victims-edge-into-light.html.

Platzer, Peter, et al. "ArduSat - Your Arduino Satellite in Space," Kickstarter, http://www.kickstarter.com/projects/575960623/ardusat-your-arduino-experiment-in-space.

"Registration of Objects Launched into Outer Space." *United Nations Office of Outer Space Affairs*. http://www.unoosa.org/oosa/en/SORegister/index.html.

"Sandy Antunes, O'Reilly Media," http://www.oreillynet.com/pub/au/4997

Seo, Michael. "NASA to Launch the First Satellites Built by High School Students" *Popular Mechanics*. March 22, 2011. http://www.popularmechanics.com/science/space/nasa/nasa-to-launch-the-first-satellites-built-by-high-school-students.

"Small Satellite Launch Opportunities on the Rise." *Space News*. Aug 13, 2012. http://www.spacenews.com/article/small-satellite-launch-opportunities-rise.

Space Exploration Technologies Corporation. "Falcon Heavy Overview." http://www.spacex.com/falcon_heavy.php.

“SpaceX to Launch Private Astronauts in 2015.” Space Industry News. Accessed May 5, 2013. http://spaceindustrynews.com/spacex-to-launch-private-astronauts-in-2015/2221/.

Surrey Satellite Technology. *Small Satellite Home Page*. http://centaur.sstl.co.uk/SSHP/sshp_classify.html

———. "World’s first 'phonesat', STRaND-1, successfully launched into orbit." Feb 25, 2013. http://www.sstl.co.uk/News-and-Events?story=2123.

Talbert, Tricia. "PhoneSat: Smart, Small and Sassy." Dec 21, 2012. http://www.nasa.gov/offices/oct/home/PhoneSat.html

Thomas Jefferson High School CubeSat Program. "Systems Engineering at TJHSST." http://tj3sat.wikidot.com

"TLS Customer Support Plan," Transmitter Location Services LLC, http://tlsglobal.com/CustomerSupportPlan.html.

“UCS Satellite Database | UCSUSA.” Union of Concerned Scientists. Accessed May 4, 2013. http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html.

Verlini, Giovanni. "The Bright Future of Small Satellite Technology." http://www.satellitetoday.com/via/features/The-Bright-Future-of-Small-Satellite-Technology_37150.html.

Weeden, Brian. "Space Situational Awareness Fact Sheet." *Secure World Foundation*. Feb 1, 2012. http://swfound.org/media/1800/ssa%20fact%20sheet.pdf

Wiens, S., and K. Epstein. “Low Cost Deployment of Auxiliary Payloads.” *IEEE Aerospace Conference Proceedings* (vol. 4, 2000): 329–334.

Yoder, Brian L. "Engineering by the Numbers." *Profiles of Engineering and Engineering Technology Colleges* (American Society for Engineering

Education, 2011). http://www.asee.org/papers-and-publications/publications/college-profiles/2011-profile-engineering-statistics.pdf.

Books

Agnew, Robert. *Why Do Criminals Offend? A General Theory of Crime and Delinquency*. Los Angeles, CA: Roxbury, 2005.

Benson, Bruce L., and Paul R Zimmerman. *Handbook on the Economics of Crime*. Cheltenham, UK; Northampton, MA: Edward Elgar, 2010.

Bernard, Thomas J. *Vold's Theoretical Criminology*. 6th ed. New York: Oxford University Press, 2010.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. London, UK: IISS, The International Institute for Strategic Studies, 2011.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Columbia University Press, 2009.

Box, George E. P. *Empirical Model-building and Response Surfaces*. Wiley Series in Probability and Mathematical Statistics (New York: Wiley, 1987).

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.

Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age*. London; New York: Frank Cass, 2005.

Eck, John E, and David Weisburd. *Crime and Place*. Vol. 4. Crime Prevention Studies. Monsey, NY: Willow Tree Press, Inc., 1995.

Felson, Marcus. *Crime and Everyday Life*. 2nd ed. SAGE Publications, Inc, 1998.

Glaser, Daniel. *Social Deviance*. Markham Publishing Company, 1974.

Gray, Colin S. *Modern Strategy*. Oxford University Press, 1999.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010.

Kramer, Franklin D., Stuart H. Starr, and Larry Wentz. *Cyberpower and National Security*. Potomac Books, Inc., 2009.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. Frank Cass, 2004.

McCurdy, Howard E. *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program*. The Johns Hopkins University Press, 2003.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs, 2012.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press, 1971.

Winter, Harold. *The Economics of Crime: An Introduction to Rational Crime Analysis*. London; New York: Routledge, 2008.

Wylie, J. C. *Military Strategy: a General Theory of Power Control*. Annapolis, Md.: Naval Institute Press, 1989.

Briefings/Memos/Messages

Bille, Matt, Tom Hunsaker, and Paul Kolodziejski. "Nanosatellite Launch Vehicles: A Global Perspective and Business Case Analysis." Presentation at the Rocky Mountain AIAA Technical Symposium. Oct 26, 2012. http://info.aiaa.org/Regions/MW/Rocky_MNT/ATS/ATS2012%20Presentations/Bille.pdf.

Graziani, Filippo. "2nd IAA Conference on University Satellites Missions and the 2nd Cubesat Winter Workshop." *International Academy of Astronautics*. http://iaaweb.org/content/view/524/695.

Wong, Hong, Christopher Wilkins, Raz Tamir, and Vikram Kapila. "A Feasibility Study of a Novel Scheme to Deploy a Constellation of Cubesats Using Two Deployers." In AIAA Guidance, Navigation and Control Conference and Exhibit. Guidance, Navigation, and Control and Co-located Conferences. American Institute of Aeronautics and Astronautics, 2007.

Government Documents

Dawson, Virginia P. and Mark D. Bowles. *Taming Liquid Hydrogen: The Centaur Upper Stage Rocket 1958-2002*. National Aeronautics and Space Administration: NASA SP-2004-4230, 2004.

Hertzfeld, Henry R. *Space Economic Data 2002*. United States Department of Commerce: Office of Space Commercialization. http://www.space.commerce.gov/library/reports/2002-12-economic-data.pdf.

Mullen, Michael G, and United States. Joint Chiefs of Staff. "The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership." 2011. http://purl.fdlp.gov/GPO/gpo4086.

National Aeronautics and Space Administration. *Launch Services Program, Program Level Poly-Picosatellite Orbital Deployer (PPOD) and CubeSat Requirements Document.* LSP-REQ-317.01 Rev A. http://www.nasa.gov/pdf/627972main_LSP-REQ-317_01A.pdf.

United States. Department of Defense. "Department of Defense Strategy for Operating in Cyberspace," 2011. http://purl.fdlp.gov/GPO/gpo10120.

United States. Department of Labor: Bureau of Labor Statistics. "Aerospace Engineers: Occupational Employment and Wages, May 2012." http://www.bls.gov/oes/current/oes172011.htm.

United States. Federal Aviation Administration. *Commercial Space Transportation: 2011 Year in Review.* January 2012.

United States. Federal Aviation Administration. *The US Commercial Suborbital Industry: A Space Renaissance in the Making.* HQ-

111460.INDD. http://www.faa.gov/about/office_org/headquarters_offices/ast/media/111460.pdf.
United States. Federal Aviation Administration: FAA Commercial Space Transportation Advisory Committee. *2012 Commercial Space Transportation Forecasts*. May 2012.

Reports

CubeSat. "CubeSat Design Specification Rev 12." 1 August 2009. http://www.cubesat.org/images/developers/cds_rev12.pdf.
Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown University Press, 2012.
Futron Corporation. *Space Transportation Costs: Trends in Price Per Pound to Orbit 1990-2000*. Sept 6, 2002. http://www.futron.com/upload/wysiwyg/Resources/Whitepapers/Space_Transportation_Costs_Trends_0902.pdf.
Gill, Martin, and Angela Spriggs. *Assessing the Impact of CCTV*. UK Home Office Research Study 292. Feb 2005.
Satellite Industry Association. *2012 State of Satellite Industry Report*. May 21, 2012. http://www.sia.org/wp-content/uploads/2012/05/FINAL-2012-State-of-Satellite-Industry-Report-20120522.pdf
Space Foundation. *The Space Report 2011: The Authoritative Guide to Global Space Activity*. Colorado Springs, CO: Space Foundation, 2011.

Speeches

Garvey, John. "The Innovator's Dilemma and the Emerging Market in CubeSat Launch Services," speech at AIAA Dinner Meeting, March 24, 2010.